State of Utah
Information Technology Resources Acceptable Use Policy

I. Purpose of State-Provided Information Technology Resources

The purpose of state-provided information technology (IT) resources (e.g., computer hardware and software, electronic communication systems, telecommunications equipment, Internet use, and future technologies) is to support state agencies in achieving their mission and goals, and to improve state government in general. These resources are intended to assist in the efficient and effective day to day operations of state agencies, including collaboration and exchange of information within and between state agencies, other branches of government and others. These resources also provide public access to public information.

Effective use of state-provided IT resources is important to the State of Utah. To help improve the effectiveness of your use of these resources, incidental and occasional personal use is permitted, (1) as long as such use does not:

- interfere with existing rules or policies pertaining to the agency,
- disrupt or distract the conduct of state business (e.g., due to volume or frequency),
- involve solicitation,
- involve a for-profit personal business activity,
- have the potential to harm the state, or
- involve illegal activities.

Note: Any resources used for personal use that incurs a cost must be reimbursed to the state.

II. Purpose of this Policy

The intent of this policy is to assure that:

1. The use of state-provided IT resources are related to, or for the benefit of, state government.
2. State-provided IT resources are used productively.
3. Disruptions to state government activities, because of inappropriate use of state-provided IT resources, are avoided.
4. The state government community is informed about confidentiality, privacy, and acceptable use of state-provided IT resources as defined in this policy.

This policy is not meant to be a straightjacket on the use of these resources. Rather, the intent is to create an environment where communication can flow freely and with a minimum of policing. This policy should not discourage the state agency from using state-provided IT resources.

Refer to the following appendices for detailed information:

- Appendix A - Responsibilities
- Appendix B - Unacceptable Use of IT Resources
- Appendix C - Overview of Technologies

III. Statutory Authority

State agencies shall comply with the policies and standards established by the Chief Information Officer (CIO). The CIO has the authority under Utah Code (§ 63D-1-301), to set policy for all state agencies except: legislative and judicial branches, State Board of Education, Board of Regents, and institutions of higher education. Any state agency may develop additional policies which may enhance this policy. The CIO has no authority over federal or local governmental entities, businesses, or individuals, except to the extent that they must agree to abide by this policy when using state-provided resources.

IV. Privacy Issues and Legal Implications

A state agency has the right to access and disclose the contents of electronic files, as required for legal, audit, or legitimate state operational or management purposes (Administrative Rule R365-4, Information Technology Security). Do not transmit personal information about yourself or someone else using State-supplied IT resources without proper authorization. The confidentiality of such material cannot be guaranteed. Email and other electronic files may be accessible through the discovery process in the event of litigation. Each of these technologies may create a "record" and therefore are reproducible and subject to judicial use.

V. Retention/Disposition of Electronic Records

Just as with any other government record, electronic records are retained or disposed of in accordance with Government Records Access and Management Act (GRAMA). Refer to GRAMA or seek counsel from the state agency's records manager for guidance in this area.

VI. Warnings/Corrective Actions

Each state agency shall review complaints or instances of unacceptable use brought to its attention. Violators are subject to corrective action and discipline (Administrative Rule R477-9-1, Department of Human Resource Management, Standards of Conduct), and may also be prosecuted under state and federal statutes.

Appendix A - Responsibilities

1. Access only files, data and protected accounts that are your own, that are publicly available, or to which you have been given authorized access.

2. Use IT resources efficiently and productively. Refrain from monopolizing systems, overloading networks with excessive data, or wasting computer time, connect time, disk space, printer paper, or other IT resources.

3. Be responsible for the use of your accounts. Under no condition should you give your passwords to another person. Guard yourself against unauthorized access to your accounts:

1. Change your passwords with regular frequency or in accordance with the state agency's policy regarding the frequency of changing passwords.
2. Do not use obvious passwords.

4. When you are away from your desk, take precautions to protect your accounts.

5. Report to the agency's appropriate authority if you:

_ receive or obtain information to which you are not entitled (Note: Also notify the owner or sender of such information),
_ become aware of breaches of security, or
_ know of any inappropriate use of state-provided IT resources.

6. Seek the advice of the authorized person responsible for any state-provided IT resource if you are in doubt concerning your authorization to access that resource.

7. Adhere to copyright law regarding use of software, information, and attributions of authorship. Upon the request of the agency, delete (from any computer) and return all state-provided software used for off-site work.

8. Conduct yourself as a representative of both the state agency and state government as a whole. As a minimum, this means that you shall not use IT resources to:

_ Distribute offensive or harassing statements, disparage others based on race, national origin, sex, sexual orientation, age, disability or political or religious beliefs.
_ Distribute incendiary statements which might incite violence or describe or promote the use of weapons or devices associated with terrorist activities.
_ Distribute or solicit sexually oriented messages or images.

Appendix B - Unacceptable Use of IT Resources

The first and foremost rule for using these technologies is:

Don't say, do, write, view, or acquire anything that you wouldn't be proud to have everyone in the world learn about if the electronic records are laid bare.

Any use of state-provided IT resources for inappropriate purposes, or in support of such activities, is prohibited (unless authorized through job responsibilities). The following list is currently considered unacceptable use of state-provided IT resources.

1. **Illegal Use.** Any use of state-provided IT resources for illegal purposes, or in support of such activities. Illegal activities shall be defined as any violation of local, state, or federal laws.

2. **Commercial Use.** Any use for commercial purposes, product advertisements or "for profit" personal activity.

3. **Sexually Explicit.** Any sexually explicit use, whether visual or textual. You shall not view, transmit, retrieve, save, or print any electronic files which may be deemed as sexually explicit.

4. **Religious or Political Lobbying.** Any use for religious or political lobbying, such as using Email to circulate solicitations or advertisements.

5. **Copyright Infringement.** Duplicating, transmitting, or using software not in compliance with software license agreements. Unauthorized use of copyrighted materials or another person's original writings.

6. **Unnecessary Use of IT Resources.** Wasting IT resources by intentionally:
_ placing a program in an endless loop;
_ printing unnecessary amounts of paper;
_ disrupting the use or performance of state-provided IT resources or any other computer system or network (for example, unauthorized world wide web pages, recurrent mass communications); or
_ storing any information or software on state-provided IT resources which are not authorized by the agency.

7. **Security Violations.** Accessing accounts within or outside the state's computers and
communications facilities for which you are not authorized or do not have a business need. Copying, disclosing, transferring, examining, renaming or changing information or programs belonging to another user unless you are given express

permission to do so by the user responsible for the information or programs. Violating the privacy of individual users by reading Email or private communications unless you are specifically authorized to maintain and support the system. Representing yourself as someone else, fictional or real.

8. **Viruses.** Knowingly or inadvertently spreading computer viruses. "Computer viruses" are programs that can destroy valuable programs and data. To reduce the risk of spreading computer viruses, do not import files from unknown or disreputable sources. If you obtain software or files from remote sources, follow proper procedures to check for viruses before use. You should adhere to any state agency-specific policy in this area.

9. **Junk Mail.** Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations.

10. **Confidential Information.** Transmitting classified information under the Government Records Access and Management Act without proper security. (2)

Appendix C - Overview of Technologies

Each of the following technologies may create an electronic record.
This is what separates these from other forms of communications such as a telephone
conversation. An electronic record is reproducible and therefore deserves special
recognition.

I. Email

Email is a major means of communication in state government, and it offers an efficient method of conducting state business. Email, as defined in this document, consists not only of the state-provided Email system, but also the act of sending and receiving Email through the Internet.

There are a number of characteristics that distinguish Email from other means of communication, such as paper records, telephones, and information stored on electronic media such as diskettes. Awareness of these characteristics should guide your use of Email.

1. **Backups.** As part of standard computing and telecommunications practices to prevent loss of data, Email systems and the systems involved in the transmission and storage of Email messages usually are "backed up" on a routine basis. This process results in copying data, such as the content of an Email message, onto storage media that may be retained for periods of time and in locations unknown to the sender or recipient of a message. The frequency and retention of backup copies vary from organization to organization. While it may be difficult and time consuming, it should be assumed backup copies of Email messages exist and can be retrieved, even though the sender or recipient has discarded his/her copy of a message.

2. **Special Status.** While password protecting your Email account is beyond usual measures taken to protect access to paper records and telephones, it does not confer a special status on Email records with respect to applicability of laws, policies, and practices.

3. **Monitoring.** In the course of their work, managers, network and computer operations personnel or system administrators may monitor the network or Email system (Administrative Rule R365-4, Information Technology Security). It should be assumed that the content of Email messages may be seen by these authorized individuals during the performance of their duties.

4. **Forgeries.** No system of communication is completely secure, including Email. Just as with paper communications, an Email message can be forged, and it can be distributed beyond the address list originally defined by its author.

5. **Viruses.** Executable files (e.g., *.exe, *.com) can be transmitted via Email. You must always check executable files attached to Email messages for viruses before they are executed on state-provided IT resources.

6. **Legal Implications.** Email and other electronic files may be accessible through the discovery process in the event of litigation.

II. Facsimile (Fax)

Fax machines, in the past, simply created a paper copy of the original message. With today's technology, this is becoming less and less true; an electronic copy may be created. The same rules governing acceptable use of other state-provided IT resources also apply to the use of fax technology. The faxed message may be "backed up" onto other storage media. As with other technologies, the content of faxed messages may be seen by authorized individuals during the performance of their duties.

Use of fax technology does not always require a password for access. Recipients should not assume that the sender is always as reported. A fax should always be perceived as a non-private communication method. Remember, anyone at the other end may read your fax.

III. Internet

The Internet provides the ability to communicate, collaborate with others and access information throughout the world. However, there is little in the way of hierarchy or control of the information available. Increased access to computers and people

all over the world also brings the availability of controversial material that may not be considered of value to an individual or the state.

Even if you are able to encrypt your data, anything you transmit over the Internet is subject to interception, reading, and copying by other people. This includes Email, personal information and passwords that are transmitted when you log into an account or log into another computer.

IV. Voice Mail

Voice mail is a means of communication that is in and of itself unique. It is similar to a telephone conversation, but it creates a "record". This should always be remembered by anyone using this technology. By the very definition of a record, the sender must remember that the message can also be saved, replayed, and shared with others that the sender did not intend. It also can be used in litigation. The same rules of password protection and confidentiality that concern other technologies also apply here.

Technologies That May Not Create Records

There are other IT resources that may not create records that are also governed by this policy. Examples of these resources include:

- various types of computer hardware and software,
- telephones,
- cellular phones,
- pagers,
- two-way radios, and
- other communications devices.

Resources such as these that are provided by the state are for the purpose of conducting state business as laid out in this policy. For details see Part I. Purpose of State-Provided

Information Technology Resources.

Emerging Technologies

This policy does not address the specific details of technologies that are yet to be invented or implemented within state government. This policy should be sufficient to allow you to determine the acceptable use of any new or emerging technology. If you have any questions regarding appropriate use of a particular technology not specifically covered in this policy, please contact the appropriate individual in the state agency.

History:

- August 15, 1996: The policy was formally adopted by the State Information Technology Policy and Strategy Committee.

- May 22, 1997: The policy was amended. The definition of state-provided information technology resources was broadened to include computer hardware, software, electronic communications systems, and telecommunications equipment. The amendment was formally adopted by the State Information Technology Policy and Strategy Committee.

1. *Your judgment regarding incidental and occasional personal use is important. While this policy does not attempt to articulate all required or proscribed behavior, it does seek to assist in such judgment by providing the above guideline. If you are unclear about the acceptable "personal" use of a state-provided resource or wish to use the resource for what may be considered as a good cause, seek authorization from the state agency's appropriate authority.*

2. *Use caution when sending classified information. Always display "CONFIDENTIAL" on the screen when sending classified information. Confirm that encryption has been enabled. Inform the recipient of the information's classification, their responsibility to keep it private, and their responsibility to dispose of it in a secure manner at the end of its retention period.*